الحماية القانونية للتوقيع الإلكتروني

–دراسة فقهية مقارنة –

عارف علي عارف*

نادية ياس البياتي**

ملخص

تميز القرن الواحد والعشرون باختراعات هائلة على المستوى التقني من أهمها وأكثرها فائدة ظهور الحاسب الآلي، الذي أصبح اليوم من لوازم الحياة المتطورة، سواءً على المستوى العام أو الخاص، وعلى الرغم من الكم الهائل من الإمكانيات التي يمكن أن يوفرها الإنترنت، إلا أنه في المقابل أفرز العديد من المشكلات القانونية التي يثيرها أثناء تبادل البيانات، أو التعاقد عبر الإنترنت، وجميعها يصب في حماية أمن المعلومات، أي حماية القانون للمعاملات التي تتم عبر شبكة الاتصالات الحديثة (الإنترنت)، ذلك لأنه لا يمكن للمعاملات التجارة الإلكترونية أن تقوم في فراغ: أي من دون ضبطها أو خضوعها لتنظيم قانوني يبين قواعد إبرامها وإثباتها وتنفيذها والمسؤلية المدنية المترتبة عليها وغيرها. لذلك لابد من وجود طرف ثالث يقوم بحماية البيانات الإلكترونية والتوقيع الإلكتروني ومنها تقنية تشفير الرسائل الإلكترونية، والتوثيق الإلكتروني. وقد اعتمد الباحث على المنهج التحليلي والذي يقوم من خلاله بتحليل النصوص القانونية المتعلقة بموضوع الحماية القانونية للتوقيع الإلكتروني، كذلك اعتمد على المنهج المقارن لدراسة التشريعات الدولية وبيان مدى تطابقها مع الفقه الإسلامي، وذلك للوصول للنتائج والحلول التي من شأنها الوصول إلى صيغة قانونية تنظم مسألة الحماية القانونية للتوقيع الإلكتروني. ومن خلال ذلك أظهرت نتائج الدراسة أن التشريعات الدولية جّرمت في نصوصها الاعتداء على البيانات الإلكترونية، معتبرة كل اعتداء على البيانات أو إفشاء الأسرار أو الاحتيال أو الإتلاف عن طريق الوسائل الإلكترونية إجرامًا يعاقب عليه وفقًا لما نص عليها القانون. كما منحت التشريعات الدولية للتوقيع الإلكتروني الحماية التقنية والمتمثلة في التشفير والتوثيق الإلكتروني.

* أستاذ قسم الفقه وأصوله، كلية معارف الوحي والعلوم الإنسانية، الجامعة الإسلامية العالمية– ماليزيا.

** محاضر في قسم القانون الخاص، كلية أحمد إبراهيم للحقوق، الجامعة الإسلامية العالمية– ماليزيا.

المقدمة

مما لاشك فيه أن انعدام الثقة والأمان يشكل نقطة ضعف عند إبرام المعاملات التجارية، لذا فإن الأمن والثقة هما الدعامتان الرئيستان اللتان يعتمد عليهما التعامل بصفة عامة سواء تم ذلك بأساليب تقليدية أم إلكترونية، وهذه الأمور يسهل توافرها في التوقيع التقليدي من خلال حضور الأطراف والتأكد من شخصيتهم بسبب ارتباط النص والتوقيع بالمرتكز الورقي المادي، ولكن قد يتعذر الإثبات من حضور الموقع فعليًا وقت التوقيع في حالة التوقيع الإلكتروني بسبب انفصال التوقيع الإلكتروني عن شخص صاحبه، ووجوده ضمن محرر يكون على وسيط إلكتروني، وربما لا تتحقق فيه الضمانات المتوفرة في السندات الورقية الموقعة، لأن التعامل الإلكتروني عبر شبكة مفتوحة (الإنترنت) يجعل من العسير على الطرف الآخر (المستقبل) لأَية معاملة إلكترونية معرفة الشخص الذي يتعامل معه،كذلك تخوف الأطراف من اختراق أنظمة المعلومات والاطلاع على مضمون الرسالة، أو تغيير محتويات الرسالة، أو فك شفرة التوقيع الإلكتروني، والاستيلاء عليه واستخدامه بدون موافقة صاحبه، مما يثير **تساؤلاً عن كيفية حماية التوقيع الإلكتروني** في ظل انتشار التعاملات عبر شبكة الإنترنت مع استحداث أساليب متطورة لاختراق هذه الشبكة، فكلما زادت المعاملات عبر الإنترنت ظهرت الحاجة الماسة إلى حماية هذه المعلومات والمحافظة على سريتها؟ وللإجابة عن ذلك، سعت كثير من التشريعات العربية والدولية كالإمارات، والأردن، ومصر، وتونس، وماليزيا، وقانون الأونسترال النموذجي، وفرنسا إلى وضع قواعد وقوانين لتأمين التبادل الأمن للمعلومات بين الأطراف عبر شبكة الإنترنت، وابتكار طرق لحماية التوقيع الإلكتروني من التزوير والغش والاستيلاء عليه، وإعطاء ثقة للمتعاملين بهذه الوسائل الحديثة، وأهم طرق الحماية هي: التشفير الإلكتروني والتوثيق الإلكتروني. ولتوضيح ذلك نقسم البحث إلى فصلين، **الأول**: نتحدث عن التشفير الإلكتروني وأهميته، وطرقه، أما **الفصل الثاني**: فنتناول التوثيق الإلكتروني وواجبات مزود خدمات التصديق مع موقف الفقه الإسلامي من حماية التوقيع الإلكتروني.

الفصل الأول: التشفير الإلكتروني وطرقه (Encryption).

المبحث الأول: تعريف التشفير الإلكتروني وأهميته.

إن مفهوم التشفير ليس حديثًا، وإنما عرف منذ زمن طويل، حيث كان يستعمل في الأغراض العسكرية، والاستخبارية، أو الدبلوماسية أو غيرها من الأغراض التي كانت تتطلب فيها توفر الأمن والسرية للمعلومات المتبادلة، إلا أنه لم يعد مقتصرًا على ما سبق ذكره، وأن ظهور شبكة الإنترنت أدى إلى زيادة الطلب أو الحاجة إلى التشفير نتيجة استخدام الشبكات المفتوحة عبر شبكة الإنترنت لنقل وتبادل المعلومات،[1] حيث تكون المعاملات التجارية عرضة لمخاطر القراصنة خصوصًا أن الرسائل الإلكترونية التي تتم عبر البريد الإلكتروني قد تحتوي على معلومات شخصية، لا يرغب أصحابها الكشف عنها، ومن هنا يُثار **تساؤل عن كيفية قيام بيئة الإنترنت بتحقيق الأمن لمستخدميها؟** وللإجابة عن ذلك سنحاول في ما يلي دراسة التشفير، وبيان جوانبه القانونية والفنية، من خلال تعريفه وطرقه وذلك على النحو الآتي.

اهتمت **الشريعة الإسلامية** بحفظ الأموال، وشرعت العقوبات الرادعة لمن يحاول التزوير، أو التغيير، أو التلاعب أو غيرها، حيث حرم الله عز وجل أكل الأموال بالحيل والطرق الملتوية وذلك في قوله تعالى ﴿**وَلا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقاً مِنْ أَمْوَالِ النَّاسِ بِالإِثْمِ وَأَنْتُمْ تَعْلَمُونَ**﴾ [البقرة: 188]. فضلاً عن ذلك أباحت الشريعة الإسلامية للإنسان الدفاع عن ماله في حالة الاعتداء عليه ولو باستعمال القوة (من قتل دون ماله فهو شهيد).[2] وبناءً عليه فإن الاعتداء على التوقيع الإلكتروني يترتب عليه مخاطر على المجني عليه بشكل خاص وعلى التجارة الإلكترونية بشكل عام، وأن استخدام هذا التوقيع في المعاملات والحقوق المالية قد يسبب سرقة الأموال وضياعها، لذلك وضعت الحماية الجنائية للتوقيع الإلكتروني والتي تتفق مع مقاصد الشريعة الإسلامية في حفظ الأموال والحقوق وحرمة الاعتداء عليها، حيث وضعت عقوبات على كل من يعتدي على أموال الناس وحقوقهم،[3] وقدرت العقوبات المناسبة لكل جريمة بحسب نوعها، وجرمها، وآثارها.

---

[1] سحر البكباشي، **التوقيع الإلكتروني** (الإسكندرية: منشأة المعارف، 2009م)، ص105.

[2] **رواه** الترمذي: **باب ما جاء فيمن قتل دون ماله فهو شهيد** (1421)، والنسائي: **من قتل دون ماله** (3550)، وأبو داود: **باب في قتال اللصوص** (4772)، **وصححه الألباني في "إرواء الغليل"** (708).

[3] للاطلاع على العقوبات في الشريعة الإسلامية. انظر: علاء الدين أبي بكر بن مسعود الكاساني، **بدائع الصنائع في ترتيب الشرائع** (بيروت: دار الفكر، ط1، ج5،1996م)، ص63./ ومحمد بن عرفة الدسوقي، **حاشية الدسوقي على الشرح الكبير** (بيروت: دار الفكر، ج3، د.ت)، ص354.

ويتضح مما سبق مدى حرص الشريعة الإسلامية على الحفاظ على أموال الناس وحقوقهم، وتعتبر كل اعتداء على حقوق الناس سواء بالتزوير أو إفشاء أسرارهم جريمة ولابد أن يعاقب عليها، وهذا ما أخذت به معظم التشريعات التي نظمت المعاملات الإلكترونية.

حيث عرف البعض **التشفير الإلكتروني** بأنه (عملية تمويه الرسالة بطريقة تخفي حقيقة محتواها وتجعلها رموزًا مقروءة تتضمن معادلات والرياضية على نص إلكتروني ينتج عنه مفتاح تشفير يجعل المعلومات غير قابلة لفك تشفيرها إلا لمن يمتلك مفتاح فك التشفير المناسب).[4]

وعرفه آخر بأنه (آلية يتم بمقتضاها ترجمة معلومة مفهومة إلمعلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس، أي يمكن إرجاعها إلى حالتها الأصلية).[5]

أما التشريعات العربية والدولية، فقد انفرد المشرّعان: المصري والتونسي في نصوصهما عن باقي التشريعات العربية الخاصة بالتجارة الإلكترونية بتعريف التشفير، بينما لم تُعّرف التشريعات العربية الأخرى التشفير في نصوصهما وإنما تطرقت إلى عملية التشفير بطريقة غير مباشرة من خلال التوقيع الإلكتروني الذي يرتكز في الأساس على مبدأ التشفير، وذلك بتحويل التوقيع إلى رموز وإشارات تعبر عن الموقع.

فعرف المشرع التونسي في المادة (5/2) من قانون المبادلات والتجارة الإلكترونية التشفير بأنه "استعمال رموز وإشارات غير متداولة تصبح بمقتضاه المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز وإشارات لا يمكن وصول المعلومة بدونها".

كما عّرف المشرع المصري في المادة (1/10) من قانون التجارة الإلكترونية التشفير بأنه "تغير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو تعديلها أو تغييرها"،[6] إلا أن قانون التوقيع الإلكتروني المصري لسنة 2004م جاء خاليًا من تعريف التشفير، مكتفيًا بتعريفه فقط بقانون التجارة الإلكترونية.

وعرف المشرع الماليزي في قانون التوقيع الرقمي التشفير وذلك في المادة (2) بأنه "مجموعة من الخوارزميات الرياضية الآمنة، التي يتم تحويل الرموز المفهومة إلى رموز غير مفهومة وذلك من خلال مفتاحين هما المفتاح العام والمفتاح الخاص".[7]

---

[4] See: Martin Hogg, Secrecy and Signatures Tuning Legal spotlight on Encryption and Electronic Commerce, The Law and the Internet a Framework for Electronic commerce, 2000, ch3, p.39.

[5] طوني ميشال عيسى، **التنظيم القانوني لشبكة الإنترنت** (بيروت: منشورات دار صادر، ط1، 2001م)، ص200.

[6] انظر: الفصل الثاني– التعريفات، قانون التجارة الإلكترونية **المصري**.

[7] انظر: قانون التوقيع الرقمي **الماليزي**.

كذلك اعتمد قانون التجارة الإلكترونية الأمريكي لسنة 2000م، التشفير بوصفه وسيلةً للتعامل في التجارة الإلكترونية خاصةً لتشفير التوقيع الإلكتروني.

أما قانون الأونسترال النموذجي للتوقيع الإلكتروني حاله حال المشرع الإماراتي تعرض إلى عملية التشفير بشكل غير مباشر وذلك من خلال التوقيع الإلكتروني ولم يتطرق إلى تعريف التشفير بشكل مباشر.

ومن خلال ما سبق ذكره، **يمكننا** تعريف التشفير بأنه عملية تقنية تعتمد على الخوارزميات الرياضية يتم تحويل نصوص الرسالة المقروءة (المفهومة) إلى نصوص رسالة غير مقروءة (غير مفهومة)، أي بتحويلها إلى رموز أو إشارات لا يستطيع أي شخص قراءتها إلا من خلال مفتاح سري يقوم بفكّ ذلك التشفير وتحويله إلى نصوص مقروءة.

ويتبين لنا من التعاريف السابقة أن عملية التشفير **تتلخص** في الآتي: تحويل النصوص المقروءة إلى نصوص غير مقروءة (مشفرة) مع إمكانية إعادة النص المشفر إلى نص عادي (مقروء) بعد فكّ التشفير بمفتاح التشفير الذي يتم إنشاؤه وفكه. ومن هنا **نتساءل ما أهمية التشفير للتوقيع الإلكتروني؟**

تبرز أهمية التشفير بعد زيادة التبادل التجاري عبر شبكة الإنترنت ووجود وسائل الاتصالات الحديثة أو ما يعرف بالتجارة الإلكترونية، وبعد أن أصبح التوقيع الإلكتروني عاملا ًمهمًا في إتمام الصفقات التجارية وغيرها من المعاملات التي تتم عبرا لإنترنت، حيث أصبح هناك ما يعرف بالقراصنة الذين يقومون بالاعتداء على الرسائل أو السيطرة على التوقيع وذلك بفكّ شفرة التوقيع الإلكتروني الخاصة بشخص آخر واستخدامه بدون موافقة صاحبه أو علمه بذلك.[8]

لذلك برزت أهمية التشفير من خلال حماية البيانات والأعمال والمراسلات والتحويلات المالية التي يتم تداولها من خلال شبكة الإنترنت، كذلك يعتبر التشفير من الدعائم الأساسية التي تقوم عليها التجارة الإلكترونية لاكتساب ثقة المستهلك وإدخال الطمأنينة عليه، وحتى لا تكون بياناته عرضة للاختراق.[9]

والحقيقة أن انتهاك سرية البيانات أو إفشائها بفكّ الشفرة الخاصة بها يمثل جريمة، لذلك اتجهت معظم التشريعات العربية والدولية كالإمارات، والأردن، ومصر، وماليزيا، وقانون الأونسترال النموذجي وغيرها، إلى تجريم الاعتداء على بيانات الرسائل، حيث اهتمت هذه التشريعات بوضع نصوص قانونية للحدِ من هذه

---

[8] انظر: جريدة أخبار العرب **الإماراتية**، العدد255، السنة الأولى، تاريخ الإصدار 2001/8/8م.

[9] لابد من**التفرقة** بين تشفير التوقيع الإلكتروني وتشفير الرسالة الإلكترونية، فالأول يقتصر على تشفير التوقيع دون بقية الرسالة، حيث يمكن أن يرتبط التوقيع المشفر برسالة غير مشفرة، في حين تشفير الرسالة الإلكترونية يتم تشفيرها بأكملها (الرسالة والتوقيع)، على الرغم من أن كليهما يقوم على عملية حسابية يتم من خلالها تشفير مضمون التوقيع والرسالة.

الجرائم ردعًا لقراصنة المعلوماتية، وللمعتدين على البيانات الخاصة بالأفراد. واعتبر كل اعتداء على البيانات أو إفشاء الإسرار أو الاحتيال أو الإتلاف عن طريق الوسائل الإلكترونية إجرامًا ويعاقب عليه وفقًا لما تنص عليه مواد القانون.

ونرى، أهمية قيام التشريعات المختلفة بفرض عقوبة على كل من يعتدي على البيانات دون إذن من طرفي العلاقة، لأن هذه الجرائم موجهة إلى عمليات التجارة التي تتم عبر شبكة دولية، كما يعد جريمة تزوير التوقيع الإلكتروني والاعتداء على البيانات أحد أهم التهديدات التي توجه إلى نمو التجارة الإلكترونية واتساع عدد مستخدميها عبر إضعاف ثقة مستخدمي تلك الوسيلة في إبرام الاتفاقات التجارية.

على الرغم من أنه مازال هناك تخوف من المتعاقدين وعدم وجود الثقة الكافية لدى المتعاملين بالمعاملات الإلكترونية، والسبب في ذلك انفصال المتعاقدين اثناء التعاقد ويتم تطبيقه آليًا أو إلكترونيًا بعكس التوقيع التقليدي (الورقي) الذي يتم بحضور الأطراف ومعرفة هوية المتعاقدين والتوقيع على المحرر بشكل مباشر.

المبحث الثاني: طرق التشفير.

هناك طريقتان أو منظومتان للتشفير والتي يبنى على أساسهما التوقيع الإلكتروني وهما:

1- التشفير عبر المفتاح السري (الخاص) أو المفتاح المتماثل (Symmetric Encryption).

تتم عملية التشفير في هذه الطريقة باستخدام كل من المرسل والمرسل إليه مفتاح تشفير واحد، الذي تم إعداده بين طرفي العلاقة ليتم التشفير من خلاله وتحويل الرسالة إلى رموز وإشارات غير مفهومة، حيث يقوم المرسل بكتابة الرسالة وتشفيرها ثم يرسل المفتاح نفسه المعد للتشفير إلى الشخص المستقبل بطريقة آمنة لفكّ التشفير، إلا أنه يعاب على هذه الطريقة انعدام السرية وإمكانية الاطلاع على محتوى الرسالة من قبل الآخرين بسبب تبادل المفتاح السري نفسه بين الطرفين من خلال إرساله عبر شبكة مفتوحة (الإنترنت)، مما يسهل الحصول عليه وفكّ عملية التشفير وتحويلها من نصوص مشفرة إلى نصوص مقروءة (مفهومة).[10]

2- التشفير عبر المفاتيح العمومية (العام) أو المفتاح غير المتماثل (Asymmetric Encryption) .

---

[10] انظر: قرطاس المنصف، **حجية الإمضاء الإليكتروني أمام القضاء– التجارة الإليكترونية والخدمات المصرفية والمالية عبر الإنترنيت** (بيروت: اتحاد المصارف العربية، 2000م)، ص248./ ومصطفى أبومندور موسى، **خدمات التوثيق الإليكتروني– تدعيم للثقة وتأمين للتعامل عبر الإنترنيت– دراسة مقارنة**، بحث مقدم إلى مؤتمر الجوانب القانونية للتعاملات الإليكترونية (مسقط: 2008م)، ص28 وما بعدها./ والأنصاري حسن النيداني، **القاضي والوسائل الإليكترونية الحديثة** (الإسكندرية: دار الجامعة الجديدة، 2009م)، ص17.

لقد ظهر هذا النوع من التشفير بوصفه بديلاً للطريقة الأولى لحل مشكلة التوزيع غير الآمن للمفاتيح في الطريقة الأولى (المتماثلة)، حيث يستخدم في هذه الطريقة مفتاحين أحدهما للتشفير يدعى المفتاح العام (Public key) والآخر بفكّ التشفير يدعى المفتاح الخاص أو المفتاح السري (Private key) ويكون المفتاحان مرتبطين رياضيًّا ويصدران من قبل نظام واحد، وفي هذا النظام يقوم المرسل بتشفير الرسالة مستخدمًا المفتاح العام (يكون هذا المفتاح معلومًا للجميع) ثم يرسلها إلى المرسل إليه فيقوم بحل التشفير بعد استلام الرسالة المشفرة بواسطة المفتاح الخاص المحفوظ لديه، والذي لا يعلمه إلا من يمتلك المفتاح الخاص أو السري (المرسل إليه) لقراءة الرسالة.

ويفهم من هذه الطريقة، أن حماية البيانات والتوقيع الإلكتروني مرتبطة إلى حد بعيد بالمفتاح الخاص أو الرقم السري والتي تعبر عن هوية صاحب التوقيع، لذا لابد أن يكون هذا المفتاح سريًّا وغير معلوم للآخرين، لضمان حماية البيانات والتوقيع الإلكتروني، ولكن يثار **تساؤل حول مدى الاعتراف بالتوقيع الإلكتروني في حالة كشف بياناته وأصبح معروفًا للجميع؟**

ولضمان الأمان في عملية التشفير لابد من وجود طرف ثالث محايد أو ما يسمى بمزود التصديق يكون موضع ثقة لدى الطرفين (كما سنرى في المبحث الآتي) ويعمل هذا الطرف على تقديم شهادات إلكترونية تبين أن المفتاح العام يقود إلى شخص صاحبه الذي يدعي أنه من قام بإرسال الرسالة وتوقيعها. وهذا ما أخذت به معظم التشريعات العربية والدولية التي نظمت المعاملات الإلكترونية كالإمارات، ومصر، والأردن، وتونس، وماليزيا، وأمريكا والأمم المتحدة بشأن التجارة الإلكترونية.[11]

وخلاصة ما سبق، فإن عملية التشفير تتم بطريقتين: الطريقة المتماثلة والطريقة غير المتماثلة وهذا الأخير يتميز بالسرية والأمان أكثر من الطريقة الأولى، بسبب وجود مفتاحين عام وخاص ويكون المفتاح الخاص سريًّا وغير معلن للأشخاص بعكس المفتاح العام يكون معلومًا للجميع، وأن وجود طرف ثالث أو ما يسمى بمزود خدمات التصديق يُعَدُّ من أهم وسائل حماية التوقيع الإلكتروني والتي من خلالها تعطيل لأطراف الثقة في التعامل الإلكتروني عبر الوسائط الإلكترونية.

[11] راجع: قانون المعاملات والتجارة الإليكترونية **الإماراتي**، الفصل الخامس بعنوان "الأحكام المتصلة بالشهادات وخدمات التصديق"./ ومدحت عبد الحليم رمضان، **الحماية الجنائية للتجارة الإليكترونية** (القاهرة: دار النهضة العربية، 2001م)، ص32.

الفصل الثاني: التوثيق الإلكتروني وواجباته (Electronic authentication).

لقد سبق القول إن تشفير البيانات والتوقيع وتحويلها إلى رموز أو إشارات تحفظ لها خصوصيتها وتجعلها بمنأى عن المساس من الغير سواء بالإطلاع أو التغيير أو التعديل، إلا أنه لم يقضِ على كل المشاكل التي تظهر في خضم الواقع العملي، وذلك لما تتسم به طبيعة هذه العقود من عدم الالتقاء الفعل يبين أطراف العلاقة، فضلاً عن ذلك عدم وجود علاقة سابقة بين الأطراف في المعاملات الإلكترونية، ولكي تتوفر الثقة والأمان لدى مستخدمي الوسائط الإلكترونية لابد من وجود طرف ثالث محايد بين أطراف التعاقد يسمى بمزود خدمات التصديق، ولتوضيح ذلك نقسم الفصل إلى مبحثين: **الأول**: تعريف مزود خدمات التصديق وواجباته، **والثاني**: شهادة المصادقة الإلكترونية مع بيان موقف الفقه الإسلامي.

المبحث الأول: تعريف مزود خدمات التصديق وواجباته (Certification service provider)

في الوقت الحاضر، أصبح العديد من المعاملات يتم رقميًا باستخدام أجهزة تقنية حديثة كالإنترنت، وقد واجهت هذه المعاملات بعض الصعوبات القانونية من حيث إثباتها وتحديد مضمونها، فالكتابة التقليدية تنعدم مع المعاملات الإلكترونية، والتوقيع التقليدي (الخطي) يختفي ليحل محله التوقيع الإلكتروني، لذا كانت الحاجة إلى طرف ثالث محايد يقوم بدور الوسيط بين الأطراف عبر تقنيات الاتصال الحديثة، حيث يقوم بالتأكد من صحة المعلومات ومصداقيتها، والتأكد من عدم العبث أو الاحتيال، ويؤمن عملية التوقيع الرقمي. ويكون الطرف الثالث (الوسيط) عبارة عن هيئة أو جهة حكومية عامة أو خاصة تصدر شهادات إلكترونية تثبت هوية الأشخاص المستخدمين لهذا التوقيع الإلكتروني، وتتبع التغيرات والأخطاء التي تحدث في السجل الإلكتروني بعد إنشائه، وتسمى هذه الجهة (بمزود خدمات التصديق)، حيث تعددت تسميات الطرف الثالث من قبل التشريعات العربية والدولية التي نظمت قانون المعاملات والتجارة الإلكترونية، ففي القانون الإماراتي أُطلق عليها اسم (مزود خدمات التصديق)، وفي القانون المصري أُطلق عليها (جهات التصديق الإلكتروني)، وفي القانون الأردني أُطلق عليها (مقدم خدمة التوثيق)، أما القانون الماليزي فقد أُطلق عليها اسم (سلطة التصديق)، وفي قانون الأونسترال النموذجي للتوقيع الإلكتروني أُطلق عليها (سلطة مقدم

التصديق)، وفي التوجيه الأوروبي أُطلق عليها (مزود خدمة التصديق)،[12] وعلى الرغم من اختلاف التسميات إلا أن جميعها تشير إلى الجهة المخولة بإصدار شهادات التصديق الإلكتروني.

ومن خلال ما ذكرناه سابقًا، نجد معظم التشريعات العربية والدولية قد اهتمتْ بمزود خدمات التصديق لتوثيق المعاملات الإلكترونية والاعتراف بحجيته، حيث عرف المشرع الإماراتي في المادة (2) من قانون المعاملات الإلكترونية مزود خدمات التصديق بأنه "أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو أيه خدمات أو مهمات متعلقة بها وبالتواقيع الإلكترونية والمنظمة بموجب أَحكام الفصل الخامس من هذا القانون".

أما القانون المصري بشأن التوقيع الإلكتروني، فقد جاء خاليًا من أي تعريف لجهة خدمات التصديق، وإنْ كان قد حظر مزاولة نشاط إصدار شهادات التصديق الرقمي، إلا بعد الحصول على ترخيص من هيئة تنمية صناعة تكنولوجي االمعلومات.

كذلك بالنسبة للقانون الأردني بشأن المعاملات الإلكترونية، حيث لم يضع تعريفًا لمقدم خدمات التصديق إلا أنه خّول مجلس الوزراء إصدار الأنظمة التي تحدد الجهة التي تشرف على تراخيص مقدم يخدمات التوثيق وإجراءات إصدار الشهادات وجميع الأمور المتعلقة بها.

أما القانون الماليزي، فقد عّرف سلطة التصديق في المادة (d/75) من قانون التوقيع الرقمي بأنه الشخص الذي يصدر الشهادات.

وعّرفه قانون الأونسترال النموذجي في المادة (2/هـ) بأنه "شخص يصدر الشهادات ويجوز أن يقّدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية".

كذلك عّرف التوجيه الأوروبي في المادة (2) مزود خدمات التصديق بأنه "الشخص الطبيعي أو الكيان القانوني الذي يصدر الشهادات أو يوفر الخدمات الأخرى المتعلقة بالتوقيعات الإلكترونية".

كما عرف جانب من **الفقه القانوني** مزود خدمات التصديق بأنه (هيئة أو مؤسسة، عامة أو خاصة تصدر شهادات إلكترونية، تكون بمثابة سجل إلكتروني يؤمّن التوقيع الإلكتروني، ويحدد هوية الموقع، ونسبة المفتاح العام إليه).[13]

---

[12] انظر: المادة (2) من قانون المعاملات والتجارة الإليكترونية **الإماراتي**، والمادة (2) من القانون **المصري** بشأن التوقيع الإليكتروني، والمادة (2) من قانون **الأردني** بشأن التجارة الإليكترونية، والمادة (75) من قانون التوقيع الرقمي **الماليزي**، والمادة (2) من قانون **الأونسترال** للتوقيع الإليكتروني، **والتوجيه الأَوروبي**.

[13] عيسى، **التنظيم القانوني لشبكة الإنترنيت**، ص205.

وعرفه آخر بأنه (شخص ثالث، يكون في الغالب، جهة عامة أو خاصة، تصدر شهادات إلكترونية عن طريق سجل إلكتروني، يحتوي على معلومات توضيحية للخصوم، ومنها اسم المستخدم وطالب الشهادة، واسم سلطة المصادقة وتاريخ صلاحية الشهادة الممنوحة).[14]

واستنادًا لما تقدم **يمكننا** تعريف مزود خدمات التصديق الإلكتروني بأنه جهة مرخصة أو معتمدة، تصدر شهادات إلكترونية عن طريق الوسائل الإلكترونية لضمان إثبات صحة البيانات الواردة في المحرر، أو بصحة نسبة التوقيع الإلكتروني للشخص الذي أَصدر هذا المحرر.

ويتضح من التعريفات سالفة الذكر أن جميعها تجعل المهمة الرئيسة لمزود خدمات التصديق الإلكترونيه هي إصدار الشهادات الإلكترونية، والقيام بأية خدمات تتعلق بتلك الشهادات أو المتعلقة بالتوقيع الإلكتروني، والهدف من هذه الشهادات تأكيد أن التوقيع الإلكتروني أو المحرر الإلكتروني صادر عمّن نسبت إليه، وأن توقيعه صحيح (وهذا ما سوف نبينه لاحقًا في المطلب الثاني).

وحسنًا ما فعل المشرع الإماراتي والمشرع الماليزي وقانون الأونسترال النموذجي والتوجيه الأَوروبي عندما عرفوا مزود خدمات التصديق، وطرق تنظيم عمله، لما لها من أهمية وخطورة من حيث تترتب عليها آثار قانونية مهمة بالنسبة للأطراف في العقود الإلكترونية، وحتى الغير الذي يعول على الشهادات المعتمدة من مزودي خدمات التصديق".

وقد ألزم مزود خدمات التصديق ببعض **الواجبات،** فالمشرع الإماراتي والتشريعات الأخرى كقانون الأونسترال النموذجي بشأن التوقيع الإلكتروني، والتوجيه الأَوروبي، والمشرع الماليزي والمصري، أوردوا في نصوصهم واجبات مزود خدمات التصديق،[15] بعكس المشرع الأردني والمشرع الفرنسي فهما قد أهملا ذلك.

ففي القوانين العربية والدولية فرضت بعض **الواجبات** التي تقع على مزود خدمات التصديق وهي كالآتي:

أولاً- على مزود خدمات التصديق: (أ)- أن يتصرف وفقًا للبيانات التي يقدمها بخصوص ممارساته.

(ب)- أن يمارس عناية معقولة لضمان دقة واكتمال كلما يقدمه من بيانات جوهرية ذات صلة بالشهادة أو مدرجة فيها طيلة سريانها. (ج)- إن يوفر وسائل يكون من المعقول الوصول إليها، وتمكن الطرف الذي يعتمد على خدماته من التأكد مما يلي: 1- هوية مزود خدمات التصديق. 2- أن الشخص المعني هويته في

---

[14] باسيل يوسف، **الجوانب القانونية لعقود التجارة الإليكترونية عبر الحواسيب وشبكة الإنترنيت والبريد الإليكتروني**، مجلة دراسات قانونية (بغداد: بيت الحكمة، 2000م)، العدد4، ص26.

[15] انظر: المادتين (9و10) من قانون **الأونسترال** بشأن التوقيع الإليكتروني، والمادتين (8و9) من **التوجيه الأَوروبي**، والمادة (27) من قانون التوقيع الرقمي **الماليزي**، والمادتين (15و16) من القانون **التونسي**، والمادتين (19 و20)من قانون التوقيع الإليكتروني **المصري**.

الشهادة لديه السيطرة في الوقت المعين على أداة التوقيع المشار إليها في الشهادة. 3- الطريقة المستخدمة في تعيين هوية الموقع. 4- وجود أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من أجلها أداة التوقيع. 5- ما إذا كانت أداة التوقيع صحيحة ولم تتعرض لما يثير الشبهة. 6- ما إذا كان للموقع وسيلة لإعطاء إشعار بموجب المادة (1/22/أوب) من هذا القانون. 7- إذا ما كانت هناك وسيلة مناسبة للإبلاغ عن الإلغاء... **ثانياً**- لتقرير ما إذا كانت أية نظم أو إجراءات أو موارد بشرية جديرة بالثقة لأغراض الفقرة (1/هـ) السابقة، يتعين الأخذ في الاعتبار العوامل الآتية: (أ)- الموارد المالية والبشرية بما في ذلك توافر الموجودات داخل منطقة الاختصاص. (ب)- مدى الثقة في أجهزة وبرامج الحاسب الآلي. (ج)- إجراءات معالجة وإصدار الشهادات وطلبات الحصول على الشهادات والاحتفاظ بالسجلات... (د)- مدى التناقض بين القانون المطبق على أعمال مزود خدمات التصديق وقوانين الإمارة".[16]

أما مسؤولية جهات التصديق الإليكتروني، فقد اهتمت التشريعات التي نظمت التجارة الإلكترونية بهذه المسألة باعتبارها ذات أهمية كبرى فيمن حال ثقة للمتعاملين في إطار المعاملات التجارية الإلكترونية، ويتمثل التنظيم القانوني لمسؤولية مزود خدمات التصديق على أنه: إذا حدثت أية أَضرار نتيجة لعدم صحةا لشهادة أو نتيجة لأي عيب فيها، يكون مزود خدمات التصديق مسؤولاً عن الخسائر التي يتكبدها كل طرف تعاقد مع مزود خدمات التصديق حول تقديم الشهادة. **أو** أي شخص اعتمد بصورة معقولة على الشهادة التي تصدر مزود خدمات التصديق. كما نصت على أن لا يكون مزود خدمات التصديق مسئوولا عن أي ضرر إذا أدرج في الشهادة بيانًا يقيد نطاق ومدى مسؤولية تجاه أي شخص ذي صلة. أو إذا اثبت بأنه لم يقترف أي خطأ أو إهمال، أو أن الضرر نشأ عن سبب أجنبي لا يد له فيه.

ويتضح مما سبق أن معظم التشريعات حدد مسؤولية مزود خدمات التصديق في حالات محددة كعدم صحة المعلومات التي تتضمنها شهادات المصادقة الإلكترونية، كما أعفى عن مزود خدمات التصديق من المسؤولية في حالة عدم احترام صاحب الشهادة لشروط استعمالها أو شروط إحداث التوقيع الإلكتروني، وفي حالة إذا لم يقترف مزود خدمات التصديق أي خطأ أو إهمال وإنما كان بسبب أجنبي لا يد له فيه، في تحمل صاحب التوقيع الإلكتروني المسؤولية تجاه ما يفرضه عليه القانون من واجبات حيال التوقيع الإلكتروني.

[16] انظر: قانون المعاملات والتجارة الإليكترونية **الإماراتي**.

المبحث الثاني: شهادات المصادقة الإلكترونية.

أسلفنا سابقًا أن مزود خدمات التصديق هو من يصدر شهادات المصادقة الإلكترونية والتي تكون مرخصة من قبل الجهات المسؤولية في الدولة بممارسة نشاطها، للتأكيد من أن التوقيع الإلكتروني هو توقيع صحيح وينسب إلى من صدر عنه، ويستوفي جميع الشروط والقواعد المطلوبة فيه باعتباره دليل إثبات يعول عليه.[17]

إن أهمية شهادات المصادقة الإلكترونية تعمل على تأكيد نسبة التوقيع إلى شخص الموقع من أجل تفادي انتحال شخصية الموقع، أو التلاعب في مضمون الرسالة، فالمرسل إليه قد لا يعرف منشئ الرسالة (الموقع)، إذا تم التعاقد من خلال الوسائط الإلكترونية، إذ يستطيع شخص آخر أن يقتحم موقعه ويقوم بالتلاعب في محتوى البيانات ثم يرسلها من جديدة، أو أن منشئ الرسالة قد ينكرها في حاله ما إذا رأى أن الصفقة لم تعد ملائمة له.[18] لذلك لابد من اشتراط تقديم شهادة تصدر من جهة محايدة وموثوق بها تؤكد هوية من ينسب إليه التوقيع، وصلاحيته عند إبرام التصرفات القانونية. لذلك سوف نبين موقف الفقه الإسلامي والتشريعات الدولية من شهادات المصادقة الإلكترونية.

ففي موقف الفقه الإسلامي، هناك نظام شبيه بنظام جهات التصديق الإلكتروني وهو ما يسمى عند الفقهاء بالشهادة على الخط (شهادات التصديق). وقد بدأ العمل بهذا النظام (الشهادة على الخط) بعد اتهام الناس فيما بينهم، وتغيرت ذمم الناس وأخلاقهم، ففي البداية كانت الكتابة، والخط، والختم حجة إثبات على صاحبها دون الحاجة إلى شهادة تؤكد حجيتها، إلا أن بعد انتشار الغش والتزوير، وكثرة تشابه الخطوط، رأى بعض الفقهاء ضرورة الشهادة على الخط لقبول الكتابة بوصفها حجةً في الإثبات.

فقد جاء في مواهب الجليل: (وقد كان يعمل في ما مضى بمعرفة الخط والختم دون بينة حتى حدث اتهام الناس).[19]

وجاء في كشف القناع: "ولا يكفي معرفة المكتوب إليه خط الكاتب ومعرفة ختمه، لأن الخط يشبه الخط والختم يمكن التزوير عليه، ولأنه نقل حكم أو إثبات فلم يكن فيه بد من إشهاد عدلين".[20]

---

[17] انظر: طارق كميل، "مقدمو خدمات المصادقة الإليكترونية- التنظيم القانوني واجباتهم ومسؤولياتهم"، **مجلة جامعة الشارقة للعلوم الشرعية والقانونية** (الإمارات: جامعة الشارقة، العدد3، مج5، 2008م)، ص244./ عبد الصبور عبد القوي علي مصري، **التنظيم القانوني للتجارة الإليكترونية** (السعودية:مكتبة القانون والاقتصاد، ط1، 2012م)، ص174.

[18] معين شواهنة، **حجية المحررات الإليكترونية في الإثبات– دراسة مقارنة**، رسالة ماجستير (فلسطين: الجامعة العربية الأمريكية، 2010م)، ص14 وما بعدها.

[19] عبد الله محمد بن محمد بن عبد الرحمن المعروف بالحطاب، **مواهب الجليل لشرح مختصر خليل** (بيروت: دار الفكر، ط2، ج6، 1978م)، ص143.

[20] منصور بن يونس بن إدريس البهوتي، **كشف القناع عن متن الاقناع** (بيروت: دار الفكر، د.ت)، ج6،ص364.

وقال القرطبي: "فاكتبوه: يعني الدين والأجل، والمراد: الكتابة والإشهاد، لأن الكتابة بغير شهود لا تكون حجة".[21]

وقال أيضًا العلامة ابن كثير: (فاكتبوه: أمر منه تعالى بالكتابة للتوثيق والحفظ).[22]

فأصبحت عندئذٍ الحاجة ماسّةً إلى شهادات إثبات على الخط بعد اتهام الناس فيما بينهم، ويعتبر الشهادة على خط المقر من أقوى صور الشهادة على الخط، وهي أن يقول الشاهدان نشهد أن هذا خط فلان، وكان مضمون الخط المشهود عليه يتضمن إقرارًا من صاحبه بشيء في ذمته، أو باستلامة لشيء من آخر،[23]وهذا يقترب كثيرًا من مفهوم مزود خدمات التصديق الإلكتروني ودورها في تصديق المعاملات الإلكترونية وبث الثقة اللازمة بين المتعاملين بالوسائل الإلكترونية، وقد أَجاز الفقهاء الشهادة على الخط، ولكن بشروط يجب الاعتداد بها، وهذا ما سنوضحه على النحو الآتي:-

فقد جاء في المبسوط: (فأما عند أبي يوسف رحمه الله، إذا أشهدتم على الكتاب والخاتم وشهدوا على ذلك أجيزه).[24]

وقال الشيخ المواق: (الشهادة على خط مقر جائزة، وقد أجمعوا على أن الخط رسم يدرك بحاسة البصر، والبصر يميز بين الخطين والشخصين، مع جواز اشتباه ذلك، فلما جوزوها في الشخص مع جواز اشتباه فيه، جازت في الخط بلا يمين، وقال ابن القاسم: (ولو شهد على خطه رجل حلف الطالب واستحق).[25]

وقال صاحب المجموع: (وينبغي لاشتراط صحة العقد وجود عدلين بمحل التسليم أو أكثر، ويكتب العقد بلغة يفهمها العاقدان وعدلان ثم يقع الختم به بعد كل ذلك، ليكون مناطًا عند التنازع).[26]

وفي كشاف القناع: (ولا يكفي معرفة المكتوب إليه خط الكاتب ومعرفة ختمه، لأن الخط يشبه الخط والختم يمكن التزوير عليه، ولأنه نقل حكم أو إثبات فلم يكن فيه بد من إشهاد عدلين).[27]

---

[21]عبد الله محمد بن أحمد الأنصاري القرطبي، **الجامع لأحكام القرآن** (القاهرة: دار الحديث، ج3، 1966م)،ص382.

[22]عبد الكريم محمد عبد الرحمن الطير، **الإثبات بالكتابة في الفقه الإسلامي– دراسة مقارنة**، رسالة دكتوراه (مصر: كلية الحقوق– جامعة القاهرة، 2000م)، ص318.

[23]محمد بن أحمد بن سهل السرخسي، **المبسوط**(بيروت: دار المعرفة للطباعة والنشر، ج18،ط2، 1986م)، ص173.

[24]محمد يوسف بن أبي القاسم العبدري الشهير بالمواق، **التاج والإكليل لمختصر خليل** (بيروت، دار الفكر،ج6، ط2، 1978م)، بهامش مواهب الجليل للحطاب، ص187.

[25]انظر:- محي الدين أبي زكريا يحي بن شرف النووي، **المجموع في شرح المهذب** (السعودية: مكتبة الإرشاد، ج9، د.ت)، ص96.

[26]البهوتي، **كشف القناع عن متن الإقناع**، ج6، ص143.

[27]أبي الفداء إسماعيل بن عمر بن كثير القرشي الدمشقي، **تفسير القرآن العظيم** (د.م: دار طيبة للنشر، ج1، 1997م)، ص416.

شروط الاعتداد بالشهادة على الخط.

لا شك أن كتابة الصكوك فيها حفظ للأموال والحقوق ولذلك جعلها بعض الفقهاء فرض كفاية، ولكن لابد من توفر مجموعة من الشروط حتى تكون الوثيقة أو الصك حجة، فهناك شروط يجب توافرها في الوثيقة ذاتها، وفي الشاهدين، وفي الكاتب نفسه.[28]

ففي الوثيقة نفسها، يجب أن تشمل البيانات التي تميز أطرافها، وصفات الشيء المشهود عليه وبيانات الشهود، وأن تحفظ في مكان مأمون لوقت الحاجة.[29]

فقد جاء في تبصره الحكام: (وينبغي للقاضي إذا شهد الشاهد عنده أن يكتب شهادته واسمه ونعته وقبيلته ومسكنه ومسجده الذي يصلي فيه والسنة والشهر الذي شهد فيه ثم يرفع ذلك عنده أو يرفعه في ديوانه).[30]

ويجوز أن تكون الوثيقة مكتوبة بخط المقر أو فيها شهادته فقط أو تكون مطبوعة أو مختومة، وفي ذلك يقول الحطاب في مواهب الجليل: (وجازت- أي الشهادة- على خط مقرٍّ سواء كانت الوثيقة بخطه أو فيها شهادته فقط).[31] كما يجب أيضًا أن يكون الخط حاضرًا عند الشهادة عليه حتى يعمل بمقتضاه ولا تقبل الشهادة في حال غيبة الوثيقة وهذا هو المعمول به. وجاء في الشرح الصغير في هذا المعنى: (ولا بد أيضًا من حضور الخط عند الشهادة عليه فلا تصح في غيبته وهذا هو الذي عليه العمل).[32]

أما الشاهدان، فيجب أن تتوافر فيها:

1- العدالة، لأن الشهادة على خط المقر كالنقل عنه ولا ينقل عن الواحد إلا اثنان.[33] جاء في الشرح الصغير: (ولابد في الشهادة على الخط من عدلين وإن كان الحق مما يثبت بالشاهد واليمين).[34]

2- أن يعرف الشاهدان الخط معرفة تامة كمعرفة الشيء المعين، فلا تقبل الشهادة على الخط إلا من فطن عارف بالخط.[35]

وفيما يتعلق بكاتب الوثيقة، فقد يكون أحد أطراف العقد، أو يكون كاتب عدل يستعين به أصحاب الشأن، وهذا هو الأولى حتى لا يحابي أحد أحدًا.

---

[28] حمدي أحمد سعد أحمد، "الشكلية في العقود الإلكترونية- دراسة مقارنة بين قوانين المعاملات الإلكترونية والفقه الإسلامي"، **مجلة كلية الشريعة والقانون** (مصر: كلية الشريعة والقانون- طنطا، 2009م)، ص126 وما بعدها.

[29] محمد بن يوسف أطفيش، **شرح كتاب النيل وشفاء العليل** (السعودية: مكتبة الإرشاد، ج3، 1985م)، ص93 وما بعدها.

[30] إبراهيم بن علي أبي القاسم بن محمد بن فرحون، **تبصرة الحكام في أصول الأَقضية ومناهج الأحكام** (مصر: مكتبة الكليات الأزهرية، ج1، د.ت)، ص56.

[31] الحطاب، **مواهب الجليل لشرح مختصر خليل**، ج6، ص187 وما بعدها.

[32] أحمد بن محمد أحمد الدردير، **الشرح الصغير على أقرب المسالك** (بيروت: دار الفكر، ج3، د.ت)، ص327 وما بعدها.

[33] السرخسي، **المبسوط**، ج18، ص173 وما بعدها.

[34] الدردير، **الشرح الصغير**، ج3، ص327 وما بعدها.

[35] الدسوقي، **حاشية الدسوقي على الشرح الكبير**، ج4، ص192.

قال القرطبي: (فاكتبوه: يعني الدين والأجل، ويقال أمر بالكتابة، ولكن المراد: الكتابة والإشهاد، لأن الكتابة بغير شهود لا تكون حجةً).[36] ويجوز لصاحب الخط والتوقيع أن يطلب الشهادة على الصك سواء كان مكتوبًا أو أنّ الذي بخطه هو توقيعه الذي يفيد إقراره على نفسه. فقد جاء في مواهب الجليل: (وجازت على خط مقّرٍ سواء كانت الوثيقة بخطه أو فيها شهادته فقط على نفسه).[37]

والشاهد الذي يقوم بالكتابة والتوثيق ينبغي أن يتمتع بالعدالة والعلم بما يكتب، وأن يكون نزيها جيد الخط، فقال ابن مفلح: (عدلاً: لأَن الكتابة موضع أمانة، حافظًا عالماً: لأَن في ذلك إعانة على أمره، وأن يكون عارفًا: لأنه إذا لم يكن عارفًا أَفسد ما يكتبه بجهله، ويستحب أن يكون ورعًا نزيهًا جيد الخط).[38]

كذلك قال القرطبي في الجامع لأحكام القرآن: (قال مالك لا يكتب الوثائق بين الناس إلا عارف بها عدل في نفسه مأمون).[39] وإن العدل الذي يقوم بالكتابة والتوثيق هو شخص آخر غير أطراف الوثيقة، حتى لا يحابي أحدهما على الآخر، فلا يكتب لصاحب الحق أكثر مما قال ولا أَقل.

ويتضح مما تقدم، أن الأحكام الخاصة بالشهادة على الخط في الفقه الإسلامي وما استند إليه الفقهاء من أدلة وما وضعوه من ضوابط للشهادة على الخط يتشابه أو يقترب من مفهوم مزود خدمات التصديق الإلكتروني التي نظمتها تشريعات المعاملات الإلكترونية، والسبب في ذلك أن الاثنين شهادتهما تمنح القيمة القانونية للمحرر والتوقيع، فضلاً عن ذلك نسبته لمن صدر عنه سواء أكان شخصًا واحدًا أم كانوا عدة أشخاص، وبناءً عليه يمكن تطبيق النظامين (الشهادة على الخط) و(مزود خدمات التصديق) لأن كليهما يهدفان إلى التأكيد من سلامة المحرر والتوقيع الإلكتروني، وكشف أي تعديل أو تغيير في بيانات المحرر أو التوقيع الإلكتروني.

كما عملت معظم التشريعات المنظمة للمعاملات والتجارة الإلكترونية على تنظيم الشهادة الإلكترونية، كالمشرع الإماراتي والأردني والمصري والماليزي وقانون الاونسترال وغيرها، حيث عمل المشرع الإماراتي على تنظيم شهادات المصادقة الإلكترونية، وعرفها في المادة (2) بأنها "شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة، ويشار إليها في هذا القانون ب(الشهادة)"، وفي القانون ذاته تناول المشرع الإماراتي في المادة (3/24) البيانات التي يجب أن تتضمنها شهادة المصادقة الإلكترونية، وهذه البيانات تتضمن: "أ- هوية مزود خدمات التصديق.

---

[36] القرطبي، **الجامع لأحكام القرآن**، ج3، ص382.

[37] الحطاب، **مواهب الجليل لشرح مختصر خليل**، ج6، ص187 وما بعدها.

[38] أبي إسحاق برهان الدين إبراهيم بن محمد بن عبد الله بن محمد بن مفلح، **المبدع في شرح المقنع** (د.م، مطبعة المكتب الإسلامي، ج1، د.ت)، ص43 وما بعدها.

[39] القرطبي، **الجامع لأحكام القرآن**، ج3، ص384.

ب- وأنّ الشخص المعين هويته في الشهادة لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في الشهادة. ج- أن أداة التوقيع كانت سارية المفعول عند تاريخ إصدار الشهادة أو قبلها. د- ما إذا كانت هناك أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من أَجلها أداة التوقيع أو الشهادة. هـ- ما إذا كانت هناك أية قيود على نطاق أو مدى المسؤولية التي قبلها مزود خدمات التصديق تجاه أي شخص".

أما القانون المصري بشأن التوقيع الإلكتروني فقد عرف شهادة التصديق الإلكتروني في المادة (1/و) بأنها "الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع"، أما بيانات شهادة التصديق فقد أحالها المشرع المصري إلى اللائحة التنفيذية التي سوف تصدر لهذا القانون بيانات شهادة التصديق الإلكتروني".[40]

أما قانون الأونسترال النموذجي بشأن التوقيع الإلكتروني فقد عرفه في المادة (2/2) بأنها "رسالة بيانات أو سجلا ًآخر يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع"، أما بخصوص محتويات هذه الشهادة فقد نصت المادة (9/ج) من ذات القانون على أن يوفر وسائل يكون الوصول إليها متيسرًا بقدر معقول حتى يتمكن من التأكد من أن الشهادة تتوافر فيها العناصر الآتية: "1- هوية مزود خدمات التصديق. 2- إن الشخص المحددة هويته في الشهادة كان مسيطرًا على أداة التوقيع في وقت التوقيع. 3- إن أداة التوقيع كانت صالحة في التاريخ الذي أصدرت فيه الشهادة أو قبله".

ومن خلال النصوص السابقة، يتبين لنا أن غرض إصدار شهادة التصديق الإلكتروني وهي الشهادة والإقرار من مزود بخدمات التصديق، بأن التوقيع الإلكتروني والبيانات الموجودة في المحرر صحيحة ومنسوبة لمصدره، وأنه مستوفى لجميع الشروط والمعايير الفنية والتقنية المنصوص عليها في القانون، وبناءً عليه يعتبر هذا التوقيع أو المحرر حجية في الإثبات ويعول عليه في المسائل المدنية والتجارية، كذلك يتضح لنا أن معظم التشريعات تتفق على عناصر أساسية يجب أن تحتوي عليها شهادة التصديق الإلكترونية والتي تصدر عن مزود خدمات المصادقة والذي يتولى جميع المعلومات الشخصية مباشرة من الشخص نفسه أو أن يحصل عليها من الغير بعد الموافقة من الشخص المعني.

[40] انظر: المادة (20) من قانون التوقيع الإليكتروني **المصري**.

الخاتمة

اهتمت الشريعة الإسلامية بحفظ الأموال، وشرعت العقوبات الرادعة لمن يحاول التزوير أو التغيير أو التلاعب أو غيرها، حيث حرم الله عز وجل أكل الأموال بالحيل والطرق الملتوية.

كما سعت كثير من التشريعات العربية والدولية إلى وضع قواعد وقوانين لتأمين التبادل الأمني للمعلومات بين الأطراف عبر شبكة الإنترنت، وأن أهم طرق حماية المعلومات والتوقيع الإلكتروني هي التشفير الإلكتروني، والتوثيق الإلكتروني.

وانفرد المشرعان: المصري، والتونسي في نصوصهما عن باقي التشريعات العربية الخاصة بالتجارة الإلكترونية بتعريف التشفير، بينما المشرع الإماراتي والأردني لم يعرفا التشفير في نصوصهما وإنما تطرق إلى عملية التشفير بطريقة غير مباشرة من خلال التوقيع الإلكتروني. وهناك منظومتان للتشفير والتي يبنى على أساسهما التوقيع الإلكتروني هما: التشفير المتماثل، والتشفير غير المتماثل، وهذا الأخير يتميز بالسرية والأمان أكثر من الطريقة الأولى، بسبب وجود مفتاحين عام وخاص ويكون المفتاح الخاص سّريًا وغير معلن للأشخاص بعكس المفتاح العام الذي يكون معلومًا للجميع.

واتجهت معظم التشريعات العربية والدولية إلى تجريم الاعتداء على بيانات الرسائل، فاهتمت التشريعات بوضع نصوص قانونية للحد من هذه الجرائم وارتداع قراصنة المعلوماتية، واعتبر كلا عتداء على البيانات أو إفشاء الأسرار أو الاحتيال أو الإتلاف عن طريق الوسائل الإلكترونية جريمةً يعاقب عليها وفقًا لما نص عليه القانون.

وتتفق الحماية الجناية للتوقيع الإلكتروني مع مقاصد الشريعة الإسلامية في حفظ الأموال والحقوق وحرمة الاعتداء عليها. حيث وضعت عقوبات على كل من يعتدي على أموال الناس وحقوقهم، وقدرت العقوبات المناسبة لكل جريمة بحسب نوعها وجسامتها وآثارها.

كما تبين أَن التشفير وحده لا ينهي كل المشاكل التي تظهر في خضم الواقع العملي، وإنما لابد من وجود طرف ثالث محايد بين أطراف التعاقد يسمى بمزود خدمات التصديق. وقد تعدد تتسميات الطرف الثالث من قبل التشريعات العربية والدولية التي نظمت قانون المعاملات والتجارة الإلكترونية.

وعرفت التشريعات المختلفة كالمشرع الماليزي، وقانون الأونسترال النموذجي، والتوجيه الأَوروبي مزود خدمات التصديق، وتطرقت إلى تنظيم عمله، بعكس المشرع المصري والأردني إذ لم يعرفا مزود خدمات التصديق ولم ينظما عمله.

ويخضع مراقب خدمات التصديق الإلكتروني لإشراف الدولة التي تقوم بتحديد القواعد والإجراءات التي تحدد عملها. وألزم مزود خدمات التصديق ببعض الواجبات، حيث أوردت التشريعات المختلفة كقانون الإمارات، وقانون الأونسترال النموذجي والتوجيه الأَوروبي والمشرع الماليزي والمصري، في نصوصهم واجبات مزود خدمات التصديق، بعكس المشرع الأردني والفرنسي إذ لم يوردا في نصوصهم واجبات مزود خدمات التصديق. كذلك حددت مسؤولية مزود خدمات التصديق في حالات محددة كعدم صحة المعلومات التي تتضمنها شهادات المصادقة الإلكترونية، ومن جانب آخر أعفي مزود خدمات التصديق من المسؤولية في حالة عدم احترام صاحب الشهادة لشروط استعمالها أو شروط إحداث التوقيع الإلكتروني.

ففي الفقه الإسلامي، استخدم نظام الشهادة على الخط بعد اتهام الناس فيما بينهم وتغيرت نفوس الناس، وخربت الذمم، وأن الأحكام الخاصة بالشهادة على الخط في الفقه الإسلامي وما استند إليه الفقهاء من أدلة وما وضعوه من ضوابط للشهادة على الخط، فإنه يمكن القول إن نظام الشهادة على الخط يتشابه مع مفهوم مزود خدمات التصديق الإلكتروني التي نظمتها تشريعات المعاملات الإلكترونية، لأن الشهادة على الخط، ومزود خدمات التصديق كلاهما يمنحان المحرر والتوقيع الإلكتروني اللذين يعول عليهما في الإثبات القيمة القانونية، ويبينان هوية الشخص (الموقع) ونسبة التوقيع إلى شخص الموقع نفسه.

كما عملت معظم التشريعات المنظمة للمعاملات والتجارة الإلكترونية على تنظيم الشهادة الإلكترونية، والبيانات التي يجب أن تتضمنها شهادة المصادقة الإلكترونية.

*** النتائج والتوصيات:**

*** النتائج:**

1- لم يعرف بعض التشريعات التشفير ومنها التشريع الإماراتي، مكتفيًا بالتطرق إلى عملية التشفير بطريقة غير مباشرة من خلال التوقيع الإلكتروني، بعكس المشرع المصري والتونسي فقد عرّفا التشفير في نصوصهما. كما تبين أَن التشفير وحده لا ينهي كل المشاكل التي تظهر في خضم الواقع العملي، وإنما لابد من وجود طرف ثالث محايد بين أطراف التعاقد يسمى بمزود خدمات التصديق.

2- جرّمت التشريعات الدولية في نصوصها الاعتداء على البيانات الإلكترونية، معتبرًا كل اعتداء على البيانات أو إفشاء الأسرار أو الاحتيال أو الإتلاف عن طريق الوسائل الإلكترونية إجرامًا يعاقب عليه وفقًا لما نص عليها القانون.

3- تتفق الحماية الجنائية للتوقيع الإلكتروني مع مقاصد الشريعة الإسلامية في حفظ الأموال والحقوق وحرمة الاعتداء عليها. حيث وضعت الشريعة الإسلامية عقوبات على كل من يعتدي على أموال الناس أو يحاول التزوير أو التغيير أو التلاعب، فقسمت العقوبة إلى حدود وتعازير.

4- عرف بعضهم مزود خدمات التصديق، وتطرق إلى تنظيم عملها، وبعضهم لم يعرف مزود خدمات التصديق ولم ينظم عملهم، وعلى الرغم من تعريفه لمزود خدمات التصديق إلا أنه مازال حتى الآن لم يطبق عمليًا على أرض الواقع.

5- إن نظام الشهادة على الخط يتشابه مع مفهوم مزود خدمات التصديق الإلكتروني التي نظمتها تشريعات المعاملات الإلكترونية، لأن كليهما يمنح الحجية القانونية للمحرر والتوقيع الذي يعول عليها في الإثبات، ويبين هوية الشخص (الموقع) ونسبة التوقيع إلى صاحبه.

*** التوصيات:**

1- تشديد الجزاءات الجنائية على الجرائم المتعلقة بالحاسب وتقنية المعلومات بخصوص عمليات السرقة والتزوير التي تتم بواسطة الحاسب الآلي، والتي توثر سلبيًّا أو تعيق انتشار التجارة الإلكترونية.

2- نوصي بإصدار تشريع عالمي موحّد تلتزم به كل الدول على شكل اتفاقية دولية بشأن حماية المعاملات والتجارة الإلكترونية باعتبار هذه المعاملات تتصف بالعالمية وليس فقط المحلية.

3- الإسراع في تفعيل التوقيع الإلكتروني وجعله متاحًا للجميع من قبل الدول لما سيسفر عنه من تكاملية وسرية وسرعة وموثوقية، مع أهمية حصول كل مواطن على توقيع إلكتروني مسجل خاص به. وأن يكون لأي مؤسسة توقيعها الخاص بها. وتغيير التوقيع الإلكتروني بعد فترة زمنية مناسبة لزيادة الأمن والحماية.

4- ضرورة نشر الوعي الثقافي والإعلامي بخصوص استخدام التوقيع الإلكتروني في العقود، من خلال وسائل الإعلام والمحاضرات والندوات الجماهيرية، وإبراز أهميته بوصفه عنصرًا فعالاً في المعاملات التجارية في العصر الحديث، مع التركيز على بعده الأمني والديني.

5- ينبغي التعامل مع التقدم التكنولوجي السريع بحذر وحيطة شديدين، وأن نتعامل معه بما يتماشى مع ديننا الحنيف وتقاليدنا الراسخة وأعرافنا المتفق عليها.

،،، والله ولي التوفيق ،،،

* **المراجع:**

أولاً: المراجع باللغة العربية:

- أحمد، حمدي أحمد سعد، 2009م، **الشكلية في العقود الإلكترونية– دراسة مقارنة بين قوانين المعاملات الإلكترونية والفقه الإسلامي**، مجلة كلية الشريعة والقانون، مصر: كلية الشريعة والقانون– طنطا.
- أطفيش، محمد بن يوسف، 1985م، **شرح كتاب النيل وشفاء العليل**، السعودية: مكتبة الإرشاد، ج3.
- البخاري، أبي عبد الله محمد بن إسماعيل بن إبراهيم، 1981م، **صحيح البخاري**، بيروت: دار الفكر، ج7.
- البكباشي، سحر، 2009م، **التوقيع الإلكتروني**، الإسكندرية: منشأة المعارف.
- بن فرحون، إبراهيم بن علي أبي القاسم بن محمد، د.ت، **تبصرة الحكام في أصول الأَقضية ومناهج الأحكام**، مصر: مكتبة الكليات الأزهرية، ج1.
- بن مفلح، أبي إسحاق برهان الدين إبراهيم بن محمد بن عبد الله بن محمد، د.ت، **المبدع في شرح المقنع**، د.م: مطبعة المكتب الإسلامي، ج1.
- البهوتي، منصور بن يونس بن إدريس، د.ت، **كشف القناع عن متن الاقناع**، بيروت: دار الفكر، ج6.
- جريدة أخبار العرب **الإماراتية**، العدد255، السنة الأولى، تاريخ الإصدار 2001/8/8م.
- الحطاب، عبد الله محمد بن محمد بن عبد الرحمن المعروف، 1978م، **مواهب الجليل لشرح مختصر خليل**، بيروت: دار الفكر، ط2.
- الدردير، أحمد بن محمد أحمد، د.ت، **الشرح الصغير على أقرب المسالك**، بيروت: دار الفكر، ج3.
- الدسوقي، محمد بن عرفة، د.ت، **حاشية الدسوقي على الشرح الكبير**، بيروت: دار الفكر، ج3.
- الدمشقي، أبي الفداء إسماعيل بن عمر بن كثير القرشي، 1997م، **تفسير القرآن العظيم**، د.م: دار طيبة للنشر، ج1.
- رمضان، مدحت عبد الحليم، 2001م، **الحماية الجنائية للتجارة الإلكترونية**، القاهرة: دار النهضة العربية.
- السرخسي، محمد بن أحمد بن سهل، 1986م، **المبسوط**، بيروت: دار المعرفة للطباعة والنشر، ج18، ط2.

- شواهنة، معين، 2010م، **حجية المحررات الإلكترونية في الإثبات– دراسة مقارنة**، رسالة ماجستير، فلسطين: الجامعة العربية الأمريكية.

- الطير، عبد الكريم محمد عبد الرحمن، 2000م، **الإثبات بالكتابة في الفقه الإسلامي– دراسة مقارنة**، رسالة دكتوراه، مصر: كلية الحقوق– جامعة القاهرة.

- عيسى، طوني ميشال، 2001م، **التنظيم القانوني لشبكة الإنترنت**، بيروت: منشورات دار صادر، ط1.

- الغرناطي، محمد بن أحمد بن جزي، 1985م، **قوانين الأحكام الشرعية ومسائل الفروع الفقهية**، د.م: عالم الفكر، ط1.

- القرطبي، عبد الله محمد بن أحمد الأنصاري، 1966م، **الجامع لأحكام القرآن**، القاهرة: دار الحديث، ج3.

- الكاساني، علاء الدين أبي بكر بن مسعود، 1996م، **بدائع الصنائع في ترتيب الشرائع**، بيروت: دار الفكر، ط1، ج5.

- كميل، طارق، 2008م، **مقدمو خدمات المصادقة الإلكترونية– التنظيم القانوني واجباتهم ومسؤولياتهم**، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، الإمارات: جامعة الشارقة، المجلد5، العدد3.

- مصري، عبد الصبور عبد القوي علي، 2012م، **التنظيم القانوني للتجارة الإلكترونية**، السعودية: مكتبة القانون والاقتصاد، ط1.

- المنصف، قرطاس،2000م، **حجية الإمضاء الإلكتروني إمام القضاء– التجارة الإلكترونية والخدمات المصرفية والمالية عبر الإنترنت**، بيروت: اتحاد المصارف العربية.

- المواق، محمد يوسف بن أبي القاسم العبدري، 1978م، **التاج والإكليل لمختصر خليل**، بيروت، دار الفكر، ج6، ط2.

- موسى، مصطفى أبو مندور، 2008م، **خدمات التوثيق الإلكتروني– تدعيم للثقة وتأمين للتعامل عبر الإنترنت– دراسة مقارنة**، بحث مقدم إلى مؤتمر الجوانب القانونية للتعاملات الإلكترونية، مسقط.

- النووي، محي الدين أبي زكريا يحي بن شرف، د.ت، **المجموع في شرح المهذب**، السعودية: مكتبة الإرشاد، ج9.

- النيداني، الأنصاري حسن، 2009م، **القاضي والوسائل الإلكترونية الحديثة**، الإسكندرية: دار الجامعة الجديدة.

- يوسف، باسيل، 2000م، **الجوانب القانونية لعقود التجارة الإلكترونية عبر الحواسيب وشبكة الإنترنت والبريد الإلكتروني**، مجلة دراسات قانونية، بغداد: بيت الحكمة، العدد4.

ثانيًا: المراجع باللغة الأنجليزية.

- Martin Hogg, Secrecy and Signatures Tuning Legal spotlight on Encryption and Electronic Commerce, The Law and the Internet a Framework for Electronic commerce, 2000.

ثالثًا: القوانين.

- القانون **الإماراتي** رقم (2) لسنة 2002م بشأن المعاملات والتجارة الإلكترونية.

- القانون **المصري** رقم (15) لسنة 2004م بشأن التوقيع الإليكتروني.

- القانون **الأردني** رقم (85) لسنة 2001م بشأن المعاملات الإليكترونية.

- التوقيع الرقمي **الماليزي** رقم (562) لسنة 1997م

- قانون (**الأونسترال**) النموذجي بشأن التوقيع الإليكتروني لسنة 2001م الصادر عن هيئة الأمم المتحدة.

- **التوجيه الأوروبي** لسنة 1999م بشأن التوقيع الإلكتروني